From:	Patrick McDonnell
To:	Hurand, Gates
Cc:	de Urioste, Alejandra; Oakland, David W.; Tomer, K. Brent; Giglio, Christopher
Subject:	Gates, Please file revised ECF #1, few more to come. TY, Patrick [Docket #86 - Supporting Exhibit(s) 1b, 1c, 1d] -- NOTICE OF MOTION TO DISMISS
Date:	Tuesday, May 22, 2018 7:44:25 AM

RE: [Docket #86 - Supporting Exhibit(s) 1b, 1c, 1d] -- NOTICE OF MOTION TO DISMISS

[Docket #86 Supporting Exhibit 1b]

Federal court opinion could impact CFTC proposed guidance on retail commodity transactions in virtual currency

by Dentons

Dentons

On May 1, 2018, United States District Court Judge James Selna in Santa Ana, California, issued an opinion that could impact proposed guidance issued by the Commodity Futures Trading Commission (CFTC) regarding retail commodity transactions involving virtual currency. The opinion is in the case of *CFTC v. Monex Credit Company, et al.*, 17-01868 (C.D. Cal.).

The court rejected the CFTC's claim that Monex, a company offering both fully paid and financed precious metal transactions to retail customers, had sold off-exchange futures contracts in violation of the Commodity Exchange Act (CEA) by failing, in connection with financed transactions, to provide "actual delivery" of the underlying metals within 28 days as required by the CEA for leveraged retail commodity transactions.

The CFTC relied on an Eleventh Circuit decision in *CFTC v. Hunter Wise Commodities, LLC*, 749 F.3d 967, 970 (11th Cir. 2014), in arguing that actual delivery requires a transfer of possession and control to the buyer.

According to the CFTC, Monex allegedly failed to do this because 1) the metals purchased in financed transactions were held in third-party depositories and were not under the direct control of the buyers, and 2) Monex retained the ability to liquidate the customers' positions in the company's sole discretion, without notice to customers, under limited circumstances, including if they failed to meet margin calls.

Judge Selna rejected the CFTC's interpretation of what constituted actual delivery, holding that Monex's arrangements with depositories and its customers satisfied this requirement. The CFTC relied on the *Hunter Wise* precedent in its proposed interpretive guidance issued in December 2017 ("Retail Commodity Transactions Involving Virtual Currency") in which the CFTC suggested that "actual delivery" of virtual currency requires a purchaser to, among other things, secure full control over the virtual currency (including the right to immediately remove the full amount purchased) and have the ability to use it "freely in commerce" within 28 days of purchase.

In light of the court's ruling in *Monex* rejecting the CFTC's actual delivery argument based on the CFTC's own interpretation of *Hunter Wise*, it is likely that if the Monex decision withstands appeal, the CFTC's proposed virtual currency guidance will need to be modified.

Dentons was one of three defense firms involved in the representation of Monex in this case and participated in the preparation of the successful motion to dismiss. The opinion is available at: https://insights.dentons.com/162/_images/General/cftc-v.-monex-et-al-mtd-decision.pdf
The CFTC's 2017 interpretive guidance is available at: https://www.cftc.gov/PressRoom/PressReleases/7664-17 Send Print Report

(1b)

[Docket #86 Supporting Exhibit 1c]

May 17, 2018

How one New York court is shaping the future of cryptocurrency regulation

by DLA Piper

DLA Piper

Two cases in a New York federal courthouse – the US District Court for the Eastern of New York – have the potential to dramatically shape the future of cryptocurrency regulation.

In one case, an EDNY judge recognized the CFTC's authority to regulate virtual currencies. In the other case, a different EDNY judge will decide whether digital tokens offered during ICOs are securities subject to SEC regulation.

On March 6, 2018, Judge Jack Weinstein of the US District Court for the Eastern of New York (EDNY) ruled that virtual currencies are commodities subject to US Commodity Futures

Trading Commission (CFTC) regulation. The ruling was issued in response to a pro se motion to dismiss in *CFTC v. McDonnell* and is the first judicial endorsement of the CFTC's long-held position that the Commodities Exchange Act (CEA) authorizes it to regulate virtual currencies.

Nearly two months later, on May 8, 2018, Judge Raymond J. Dearie of the EDNY heard oral arguments in a different case – the criminal prosecution of Maksim Zaslavski – where the defendant is challenging the government's position that digital tokens offered through initial coin offerings (ICOs) are securities. While this case was brought by the US Department of Justice (DOJ), the issue has significant implications for the US Securities and Exchange Commission (SEC), which has brought parallel civil proceedings against Zaslavskiy in the EDNY and asserted broad regulatory authority over ICOs on the theory that cryptocurrencies are securities.[1]

These issues of first impression have far-reaching implications for the cryptocurrency regulatory landscape and may impact enforcement actions in the pipeline.

McDonnell decision affirming CFTC authority

On January 18, 2018, the CFTC filed a complaint accusing Patrick K. McDonnell and CabbageTech, Corp. of fraud and misappropriation in connection with the purchase and trading of two cryptocurrencies – Bitcoin and Litecoin – and the failure to provide purported "virtual currency trading advice," such as "entry and exit prices for day trading of certain virtual currencies." According to the CFTC, the defendants "used their fraudulent solicitations to obtain and then simply misappropriate customer funds." McDonnell responded with a pro se motion to dismiss the charges that challenged the CFTC's "enforcement jurisdiction."

In its response to the motion to dismiss, the CFTC directed the court to a prior filing in which it argued that virtual currencies are commodities. The CFTC asserted that the CEA's "definition of commodity is expansive in scope" and extends to "intangible commodities" ranging from "renewable energy credits and emissions allowances" to virtual currencies. As explained by the CFTC, "virtual currencies . . . fall within the [CEA's] category of 'all other goods and articles'"and "the rights and interests that inhere to each unit of virtual currency constitute 'rights [or] interests . . . in which contracts for future delivery are presently . . . dealt in.'"

The Chicago Mercantile Exchange filed an *amicus curiae* letter in support of the CFTC's virtual-currencies-are-commodities argument, cautioning that "a determination that a virtual currency such as Bitcoin is not a commodity . . . . would put in jeopardy [the Chicago Mercantile Exchange] and its market participants' expectation to rely on the CEA and the CFTC's regulatory protections for commodity derivatives contracts based on virtual currencies." The Chicago Mercantile Exchange has offered a Bitcoin futures product for trading since December 18, 2017.

In the first federal court decision affirming the CFTC's authority to regulate virtual currencies, Judge Weinstein rejected McDonnell's jurisdictional challenge He concluded that the CFTC has the authority to regulate virtual currencies. In his March 6, 2018 order, Judge Weinstein explained, "[v]irtual currencies can be regulated by CFTC as a commodity" because they "are goods exchanged in a market for a uniform quality and value" and "fall within the CEA's definition of 'commodities' as 'all other goods and articles . . . in which contracts for future delivery are presently or in the future dealt in.'" The order did not differentiate between "digital coins" – such as Bitcoin and Litecoin – that use and operate on their own platforms, and "digital tokens" – such as those at issue in the *Zaslavskiy* case – which are built on top of existing blockchain and typically represent an asset or utility. McDonnell did not draw this distinction in his pro se filing, and we predict this issue will be raised in a future CFTC case.

In his decision, Judge Weinstein left the door open to concurrent regulation by other government regulators, noting that "[t]he jurisdictional authority of [the] CFTC to regulate virtual currencies as commodities does not preclude other agencies from exercising their regulatory power when virtual currencies function differently than derivative commodities." As a result, in Judge Weinstein's view, other government bodies – including the SEC, the DOJ, the US Department of the Treasury, and the Internal Revenue Service as well as state agencies – can seek to regulate virtual currencies "without displacing CFTC's concurrent authority." As the *Zaslavskiy* prosecution and other enforcement actions demonstrate, these regulators have not hesitated to assert their authority.

***Zaslavskiy* proceedings challenging SEC jurisdiction.**

Last fall, the DOJ and SEC brought parallel proceedings against Maksim Zaslavskiy for securities fraud in connection with two ICOs. In its September 2017 complaint, the SEC alleged that Zaslavskiy's companies – RECoin Group Foundation, LLC (RECoin) and DRC World, Inc. (DRC) – sold digital tokens in a pair of ICOs that qualified as unregistered offerings of securities and that Zaslavskiy made false or misleading representations and omissions in connection with both token sales.

In October 2017, the DOJ filed a criminal complaint charging Zaslavskiy with securities fraud conspiracy for similar misconduct – engaging in illegal unregistered securities offerings and making material misstatements to deceive investors in connection with the ICOs. Federal prosecutors accused Zaslavskiy of marketing RECoin as "The First Ever Cryptocurrency Backed by Real Estate" and touting DRC as an "exclusive and tokenized membership pool" that was hedged by physical diamonds despite knowing that "no real estate or diamonds were actually backing the investments." The SEC suit was stayed pending the outcome of the DOJ action.

In February 2018, Zaslavskiy filed a motion to dismiss the criminal case, arguing that securities laws do not apply to cryptocurrencies and that Zaslavskiy's token sales do not

constitute "investment contracts" under the Supreme Court's *Howey* test – the long-recognized standard for determining if an investment instrument is a security. Zaslavskiy also argued that securities laws are void for vagueness as applied to cryptocurrency and token sales.

Both the DOJ and the SEC opposed Zaslavskiy's motion. The DOJ characterized Zaslavskiy's brief as a failed attempt to recast REcoin and DRC tokens as "currencies" rather than securities, while both tokens constituted "prototypical investment contract[s]" under *Howey*. The SEC agreed, characterizing Zaslavskiy's token ICOs as "old-fashioned fraud dressed in a new-fashioned label." Both regulators encouraged the court to focus on the economic reality of the investments as they were advertised – rather than the terminology – to evaluate the character of the token offerings.

Zaslavskiy responded by accusing the government of "advanc[ing] a vision of nearly limitless regulatory jurisdiction by the SEC" and requesting "carte blanche to regulate industries whether it has the legal authority to do so or not." Zaslavskiy challenged the government's interpretation of *Howey* as applied to REcoin and DRC, arguing that the regulators failed to satisfy two prongs of the four-prong test. In addition, Zaslavskiy warned of a "regulatory agency goldrush" in which "every American regulatory agency that has considered its jurisdiction of cryptocurrencies has concluded it has the authority to regulate cryptocurrencies."

During a hearing last week, Judge Dearie expressed uncertainty about how to treat digital tokens but was openly critical of Zaslavskiy's conduct, which he characterized as a "grand misrepresentation." At one point, the judge read from Zaslavskiy's marketing materials, which promised investors profits based on the tokens being backed by real estate assets, and observed that the language "sounds like an investment contract." When Zaslavskiy's attorney noted that Judge Weinstein recently concluded that cryptocurrencies are commodities subject to CFTC regulation, Judge Dearie suggested – similar to his colleague – that digital tokens could be subject to concurrent jurisdiction by multiple regulators. While Judge Dearie has yet to rule on the motion to dismiss, the questions reportedly posed during oral argument suggest that his decision will include an analysis of whether the tokens at issue satisfy the *Howey* test.

Impact on future cryptocurrency enforcement

Regulators have turned up the heat on cryptocurrency companies in recent months, issuing subpoenas, document requests, and cease-and-desist orders. Examples include a December 2017 enforcement action to halt a $15 million ICO by a California-based social-networking restaurant review app, a January 2018 enforcement action to halt a Texas-based bank from proceeding with an ICO and an April 2018 enforcement action against the co-founders of a financial services startup for an allegedly fraudulent ICO that raised more than

$32 million.

The *McDonnell* cryptocurrencies-are-commodities ruling allows the CFTC to assert jurisdiction over companies engaged in "pump-and-dump" schemes and other forms of market manipulation. Meanwhile, a *Zaslavskiy* cryptocurrencies-are-securities finding may embolden federal regulators to look increasingly beyond instances of egregious conduct and expand their focus on registration issues – a potential tripwire for hundreds of companies that have launched, or plan to launch, ICOs without complying with SEC registration requirements or conducting offerings that are exempt from those requirements. As noted by SEC Cyber Unit Chief Robert Cohen at a securities conference last week, the SEC is currently investigating a number of ICOs for "purely registration issues."

The *McDonnell* and *Zaslavskiy* actions are initial cases where **government regulators are testing their jurisdictional theories**. They will help chart the course for future CFTC and SEC enforcement in an industry where the law has struggled to keep pace with technology.

An earlier version of this alert appeared on Law360 on May 16, 2018.

---

1 *See* SEC Chairman Jay Clayton, "Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission," U.S. Senate Committee on Banking, Housing, and Urban Affairs (Feb. 6, 2018), *available here* ("I believe every ICO I've seen is a security"); *but see* SEC Director of the Division of Corporation Finance, "Oversight of the SEC's Division of Corporation Finance" U.S. House of Representatives Financial Services Committee (Apr. 26, 2018), *available here* (remarking in an exchange with Rep. Tom Emmer (R- MN6) that some utility tokens on decentralized networks may not qualify as securities). [View source.]

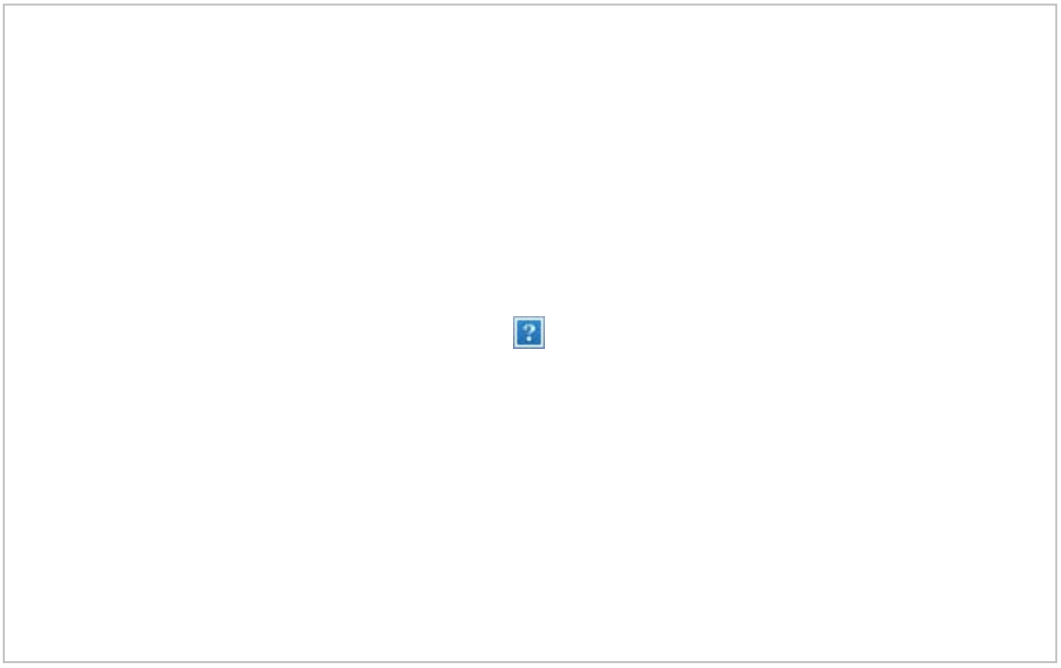
Send Print Report

(1c)

[Docket #86 Supporting Exhibit 1d]

CFTC Division of Enforcement Trends

By Elizabeth Lan Davis and Brian Walsh – 5.8.18



This piece was co-authored by Elizabeth Lan Davis, a former chief trial attorney at the Commodity Futures Trading Commission (CFTC), who joined Murphy & McGonigle a few weeks ago, and another lawyer at the Firm, Brian Walsh.

On November 22, 2017, the Division of Enforcement ("Division") of the Commodity Futures Trading Commission ("CFTC") released its annual enforcement results, announcing that it had filed 49 enforcement actions for Fiscal Year 2017. Despite the unexpected decrease to the CFTC's budget, the agency's enforcement program is on pace to markedly improve upon the number of filings made during Fiscal Year 2017. Since announcing the results, the Division has filed 29 actions thus far in Fiscal Year 2018. While the Division continues to bring cases related to fraud in off-exchange foreign currency, binary options, and precious metals, its recent foray into fraud actions involving virtual currency will likely continue to expand, along with a focus on the areas of spoofing, manipulation, and cybersecurity. In so doing, the Division will continue its close coordination with the U.S. Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC"). As the Division recently issued an enhanced advisory on self-reporting and full cooperation, subsequent filings will provide more detailed insight and guidance into the Division's expectations and the potential benefits of cooperation with the Division.

Virtual Currency

Policing fraud is one of the cornerstones of the Division's mission, and the Division has extended its reach to the virtual currency realm. The cases filed by the Division, as well as the recent decision in *CFTC v. Monex*, raise numerous issues. As detailed in our firm's Cryptocurrency Regulatory Developments overview, several earlier speaking orders issued by the CFTC indicated that Bitcoin is a commodity; however, it remains to be decided whether other virtual currencies will also be considered commodities as defined in the Commodity Exchange Act. In *CFTC v. My Big Coin Pay, et al.*, No. 18-cv-10077 (D. Mass. filed Jan. 16, 2018), the CFTC charged certain individuals and My Big Coin Pay, Inc. ("MBC"), with fraud and misappropriation in connection with alleged solicitation of customers for a virtual currency known as My Big Coin. MBC filed a motion to dismiss the CFTC's complaint and an opposition to the CFTC's motion for a preliminary injunction, arguing that the CFTC lacked jurisdiction over My Big Coin. MBC argued that the term "commodity" is defined in the Commodity Exchange Act to include, in addition to certain agricultural products, all goods, services, rights and interests "in which contracts for future delivery are presently or in the future dealt in." MBC took the position that the CFTC lacked jurisdiction because, unlike Bitcoin, there are no futures contracts traded on My Big Coin, and for that reason, it is not a commodity. The court's decision regarding MBC's argument will have a significant impact on the scope of future CFTC enforcement actions vis-à-vis virtual currency.

In addition to *My Big Coin Pay*, the CFTC filed:

-

CFTC v. Dillon Michael Dean and The Entrepreneurs Headquarters Limited, No. 18-cv-345 (E.D.N.Y. filed Jan. 18, 2018)

The CFTC alleged that, from approximately April 2017 through the time of filing of the complaint, the unregistered defendants engaged in a fraudulent scheme through which they solicited at least $1.1 million worth of Bitcoin from more than 600 members of the public. The CFTC asserted that the defendants promised to convert customers' Bitcoin into fiat currency to invest on their behalf in a pooled investment vehicle for trading commodity interests, including trading binary options on an online exchange. The CFTC alleged that potential customers were solicited to invest through false claims of trading expertise and promises of high rates of return, and that rather than converting customers' Bitcoin to fiat currency to invest in binary options contracts as promised, the defendants misappropriated their customers' funds to pay other customers.

- *CFTC v. Patrick K. McDonnell and Cabbagetech Corp. d/b/a Coin Drop Markets*, No. 18-cv-361 (E.D.N.Y. filed Jan. 18, 2018)

The CFTC alleged that, from approximately January 2017 through the time of filing of the complaint, McDonnell and Coin Drop Markets ("CDM") engaged in a deceptive and fraudulent virtual currency scheme to induce customers to send money and virtual currencies to CDM, purportedly in exchange for real-time virtual currency trading advice and for purchasing and trading virtual currency on behalf of customers under McDonnell's direction. Rather, the CFTC claimed, the defendants did not provide advice and customers did not receive refunds. The CFTC asserted that McDonnell and CDM fraudulently solicited customers to misappropriate customer funds, and then severed contact with customers and removed their web presence after funds were received.

CFTC v. Blue Bit Banc, et al., No. 18-cv-2247 (E.D.N.Y. filed Apr. 16, 2018)

The CFTC alleged that, since at least April 2014 and continuing through the time of filing, the defendants solicited potential customers through various means to purchase illegal off-exchange binary options and falsely claimed that customers' accounts would generate significant profits based upon an individual defendant's purported past profitable trading. The complaint claimed that the defendants misappropriated a substantial amount of the customer funds for their own personal use and sought to conceal the misappropriation by inviting customers to transfer their binary options account balances into a virtual currency known as "ATM Coin." The CFTC averred that some customers transferred their funds into ATM Coin, and at least one customer sent defendants additional money to purchase more ATM Coin. It was also asserted that the defendants misrepresented to customers that their ATM Coin holdings were very valuable. The day after the CFTC's filing, the court entered a Statutory Restraining Order freezing defendants' and relief defendant's assets, among other relief.

The CFTC has jurisdiction over retail commodity transactions entered into or offered to retail market participants on a leveraged or margined basis, or financed by the offeror, unless the

contracts of sale result in "actual delivery" of the commodity within 28 days of the transaction. On December 20, 2017, the CFTC issued proposed interpretative guidance on "actual delivery" of virtual currency in retail transactions, which contained "two primary factors necessary to demonstrate 'actual delivery' of retail commodity transactions in virtual currency." Those factors included: (1) a customer having the ability to (i) take possession and control of the entire quantity of the commodity, whether it was purchased on margin, or using leverage, or any other financing arrangement, and (ii) use it freely in commerce (both within and away from any particular platform) no later than 28 days from the date of the transaction; and (2) the offeror and counterparty seller (including any of their respective affiliates or other persons acting in concert with the offeror or counterparty seller on a similar basis) not retaining any interest in or control over any of the commodity purchased on margin, leverage, or other financing arrangement at the expiration of 28 days from the date of the transaction.

Notably, on May 1, 2018, the U.S. District Court for the Central District of California granted the defendants' motion to dismiss the CFTC's complaint in *CFTC v. Monex Credit Company, et al.*, No. 8:17-cv-01868 (C.D Cal.), which may influence the CFTC's definition of "actual delivery" for retail transactions in virtual currency. *Monex* involved a precious metals dealer offering retail customers precious metals on a leveraged, margined, or financed basis, where the defendant acted as the counterparty to each trade. Monex required customers to sign account agreements that gave control over the metals traded on its platform to Monex. Customers did not take physical delivery of the metals, which were stored in depositories subject to contracts between Monex and the depositories. Customers could take physical possession of the metals if they made full payment and coordinated delivery.

When the customers entered into long or short metals transactions, Monex transferred the ownership interest to the customer, a transfer which the CFTC alleged was simply a "book-entry." In deciding Monex's motion to dismiss, the court found that Monex's alleged practice of delivering precious metals to independent depositories within 28 days of purchase by retail customers on margin fell within the "actual delivery" exception, and therefore, the CFTC lacked jurisdiction to bring claims related to leveraged metals transactions. The court also dismissed the remaining count alleging fraud in violation of Section 6(c)(1) of the Commodity Exchange Act and interpreted the statute's prohibition of "manipulative or deceptive devices" to prohibit actual or potential market manipulation, and not mere allegations of fraud that had been pled in the CFTC's complaint. It will be interesting to watch the Division's approach to cases involving virtual currencies as retail commodity transactions while it likely appeals the decision in *Monex*, as well as how the CFTC will reconcile the *Monex* court's interpretation of "actual delivery" for retail commodity transactions with its proposed interpretative guidance for retail transactions in virtual currency.

Nevertheless, as the use of virtual currency becomes increasingly widespread, a probable influx of leads and referrals to the Division will increase the number of investigations and

enforcement actions. Indeed, the CFTC's Whistleblower Office recently announced a bounty program for pump and dump schemes in virtual currency, which may result in more tips and leads to the Division. Furthermore, the recent listing of bitcoin futures on CME and CBOE, along with the increase in crypto index funds, will likely draw closer scrutiny by the Division into potential registration issues. Those offering to trade bitcoin futures should consider whether registration may be appropriate. Finally, the Division will also likely be on the lookout for patterns of manipulative activity used in the traditional commodities space that are applied in the virtual currency markets.

Spoofing

Spoofing is the disruptive trading practice of bidding or offering with the intent to cancel bids or offers before execution. On January 29, 2018, the Division's Director announced eight separate actions alleging spoofing activity by three corporate entities and six individuals, and stated that the Division "will work hard to identify and prosecute the individual traders who engage in spoofing, but we will also seek to find and hold accountable those who teach others how to spoof, who build the tools designed to spoof, or who otherwise aid and abet the wrongdoing." The civil complaints filed by the Division against the individual traders, summarized below, were brought in conjunction with criminal complaints brought by DOJ, which was billed as "the largest futures market criminal enforcement action in Department history."

- *CFTC v. Andre Flotron*, No. 3:18-cv-00158 (D. Conn. filed Jan. 26, 2018)

The CFTC alleged that, from July 2011 through November 2013, Flotron engaged in a manipulative and deceptive scheme by spoofing on an ongoing basis in gold and silver futures contracts traded on COMEX.

The CFTC's complaint claimed that, on numerous occasions, Flotron placed a visibly small order for COMEX gold or silver futures contracts that he wanted to get filled and entered a larger order for the same contract on the opposite side of the book that he intended to cancel before execution. In placing the spoof orders, the CFTC claimed that Flotron intentionally sent false signals of increased demand or increased supply designed to trick other market participants into executing against his genuine orders, or that he recklessly disregarded that the spoof orders would send such false signals to market participants. The CFTC's civil case has been stayed pending the resolution of the parallel criminal proceeding, in which a jury recently found Flotron not guilty on the charge of conspiracy to commit commodities fraud. *See United States v. Flotron*, No. 3:17-cr-00220 (D. Conn. Apr. 25, 2018). The stay of the CFTC's civil case will be lifted on May 11, 2018.

- *CFTC v. Jitesh Thakkar and Edge Financial Technologies, Inc.*, No. 1:18-cv-00619 (N.D. Ill. filed Jan. 28, 2018)

The CFTC alleged that Thakkar and his company, Edge Financial Technologies, Inc. ("Edge"), aided and abetted spoofing and a manipulative and deceptive scheme in the E-mini S&P 500 futures near month contract ("E-mini S&P) listed on CME. The complaint claimed that a trader who cooperated with the Division's investigation had asked Thakkar and his company to design and develop a custom trading software application containing a function called "Back of Book" to assist the trader in placing orders that were intended to be canceled before execution. The trader allegedly engaged in thousands of occasions of spoofing from January 30, 2013 through October 30, 2013. The complaint asserted that Thakkar and Edge understood that the trader would use the function to engage in spoofing and to inject false information into the market regarding supply and demand for the E-mini S&P contract, and therefore they aided and abetted the trader's spoofing and manipulative and deceptive scheme. A parallel criminal proceeding was brought against Thakkar for conspiracy. *See United States v. Thakkar,* No. 1:18-cr-00036 (N.D. Ill. filed Jan. 19, 2018). The CFTC's civil case has been stayed in its entirety pending the resolution of the criminal proceeding or further order of the court.

- *CFTC v. Jiongsheng Zhao*, No. 1:18-cv-00620 (N.D. Ill. filed Jan. 28, 2018)

The CFTC alleged that, from at least July 2012 through at least March 2017, Zhao repeatedly engaged in a manipulative and deceptive scheme by spoofing on approximately 2,300 occasions in the E-Mini S&P futures contract listed on CME. Trading manually, Zhao allegedly intended to cancel the spoof orders before execution and often did so after his genuine orders were filled. By engaging in this scheme, the complaint claimed that Zhao entered the spoof orders either to intentionally send a false signal to the market or that he recklessly disregarded the fact that the spoof orders would inject false information about supply and demand that could affect market activity.

The initial status conference currently is scheduled for June 28, 2018. *See also United States v. Zhao*, No. 1:18-cr-00024 (N.D. Ill. filed on Jan. 11, 2018) (charging wire fraud, commodities fraud, and spoofing on CME between July 2012 and March 2016, and making false statements to CME after being confronted with allegations of his disruptive trading practices).

- *CFTC v. James Vorley and Cedric Chanu*, No. 18-cv-00603 (N.D. Ill. filed Jan. 26, 2018)

The CFTC alleged that, beginning in at least May 2008 and continuing through at least July 2013, Vorley and Chanu, while employed at a large global banking and financial services company, engaged in a manipulative and deceptive scheme by spoofing in gold, silver, platinum, and palladium futures contracts traded on COMEX. The CFTC's complaint included communications from other traders at the financial institution where Vorley and Chanu worked and alleged that Vorley and Chanu taught other traders how to spoof. The civil lawsuit currently is stayed until July 2, 2018, in light of the parallel criminal prosecution

against Vorley and Chanu. *See United States v. Vorley*, *et al.,* No. 1:18-cr-00035 (N.D. Ill. filed Jan. 19, 2018) (charging conspiracy, wire fraud, commodities fraud, and spoofing offenses in connection with executing scheme to defraud involving both solo and coordinated spoofing on COMEX).

- *CFTC v. Krishna Mohan*, No. 4:18-cv-00260 (S.D. Tex. filed Jan. 28, 2018)

The CFTC alleged that Mohan engaged in a manipulative and deceptive scheme by spoofing on tens of thousands of occasions in the E-mini Dow futures contract traded on CBOT and the E-Mini NASDAQ 100 futures contract traded on the CME from November 25, 2013 to December 17, 2013, while employed as a programmer and trader at a Chicago proprietary trading firm. The complaint claimed that Mohan concealed the size of his genuine orders by placing iceberg orders and further disguised his activity to the market by using an order splitter tool to place multiple spoof orders all at once. The CFTC's complaint also stated that Mohan carried out his scheme nearly 95% of the time during overnight sessions when trading volume and volatility were substantially decreased, and that trading overnight was a key component of his scheme and indicative of his wrongful intent. The complaint also noted that Mohan's Google Drive folder contained documents describing certain spoofing strategies. A parallel criminal proceeding was filed on January 26, 2018, charging commodities fraud and spoofing offenses by engaging in a pattern of spoofing over a thousand times. *See United States v. Mohan*, No. 4:18-mj-00080 (S.D. Tex. filed Jan. 26, 2018).

Since the announcement of these coordinated actions, the government's anti-spoofing regime has been met with mixed results. The program gained traction with the affirmation of the conviction of Michael Coscia by the Seventh Circuit, which has since been appealed to the Supreme Court. The government, however, suffered a setback with the recent acquittal in *Flotron*. The *Flotron* acquittal highlights the difficulties in proving intent, especially to a jury, as the Division's spoofing actions often rely heavily upon circumstantial evidence and trading data. Despite the acquittal in *Flotron,* which will likely be appealed, the Division will continue to bring anti-spoofing actions on behalf of the CFTC and in conjunction with the DOJ.

As such, traders should be cognizant of potential criminal liability when engaging in trading that could be potentially viewed as spoofing or otherwise disruptive.

In addition to the lawsuits described above, the January administrative settlements against corporate entities detailed the self-reporting and cooperation that resulted in "substantial" reductions in the amount of civil monetary penalties. The speaking orders in these cases provided additional color on the Division's expectations for obtaining cooperation credit. Such efforts included undertaking internal reviews and analysis that proactively assisted the Division's investigation, detecting and deterring similar misconduct in monitoring and

surveillance systems, enhancing training and policies, as well as promptly notifying the Division of the misconduct. The speaking orders, however, did not discuss what the penalties would have been in the absence of cooperation and self-reporting, thereby making it difficult to effectively gauge the benefits of self-reporting and cooperation.

The administrative settlements filed thus far in Fiscal Year 2018 are:

- *In re UBS AG*, CFTC Dkt. No. 18-07 (Jan. 29, 2018)

The CFTC found that, from January 2008 through at least December 2013, UBS AG ("UBS"), by and through the acts of certain precious metals traders on its spot desk, attempted to manipulate the price of precious metals futures contracts traded on COMEX, including gold and silver, by utilizing a variety of manual spoofing techniques. The CFTC also found that, between December 2009 through February 2012, one of UBS's traders attempted to manipulate the price of precious metals futures contracts by trading in a manner to trigger customer stop-loss orders. The order quoted several examples from communications between traders discussing their spoofing stop-loss manipulation strategies. Recognizing UBS's self-reporting of the misconduct, cooperation, and proactive remedial steps, the CFTC imposed a "substantially reduced" civil monetary penalty in the amount of $15 million.

- *In re Deutsche Bank AG and Deutsche Bank Securities Inc.*, CFTC Dkt. No. 18-06 (Jan. 29, 2018) The CFTC found that, from at least February 2008 through September 2014, Deutsche Bank AG ("DB"), by and through certain of its precious metals traders, utilized a variety of manual spoofing techniques in an attempt to manipulate the price of gold, silver, platinum, and palladium futures contracts traded on COMEX. The order also found that DB traded in a manner to trigger customer stop-loss orders by coordinating with another precious metals trader at another large financial institution from December 2009 through February 2012, and included examples from communications between the traders discussing their trading activity. In conjunction with this activity, the CFTC found that Deutsche Bank Securities Inc. failed to diligently perform its supervisory duties by failing to follow up on the majority of potential instances of misconduct identified by its electronic surveillance system. In recognizing DB's "substantial cooperation" and proactive remedial steps, the CFTC imposed a "substantially reduced" penalty in the amount of $30 million.

- *In re HSBC Securities (USA) Inc.*, CFTC Dkt. No. 18-08 (Jan. 29, 2018)

The CFTC found that HSBC Securities (USA) Inc. ("HSBC"), from July 16, 2011 through August 2014, by and through one of its traders in its New York office, engaged in numerous acts of spoofing with respect to futures contracts in gold and other precious metals traded on COMEX. Acknowledging HSBC's cooperation throughout the Division's investigation, the CFTC imposed a "substantially reduced penalty" in the amount of $1.6 million.

In re Anuj C. Singhal, CFTC Dkt. No. 18-11 (Apr. 9, 2018)

The CFTC found that a registered floor broker frequently engaged in spoofing activity through manual trading in the CME wheat futures market between at least March and June 2016. The CME previously fined Singhal in the amount of $60,000 and imposed a three-month trading suspension. The CFTC imposed a $150,000 civil monetary penalty and a four-month ban on trading all commodity interests.

- *In re Arab Global Commodities DMCC*, CFTC Dkt. No. 18-01 (Oct. 10, 2017)

The CFTC found that, from March and August 2016, at least one trader from a proprietary trading firm engaged in spoofing activity in the COMEX copper futures contract. The trader generally spoofed after business hours from home and in certain instances, used another trader's account to hide his spoofing activity. The order noted that the firm did not have an anti-spoofing policy, had not trained its traders or managers with respect to the prohibitions against spoofing in the Commodity Exchange Act and exchange rules, did not monitor the trader's COMEX trading, and did not adequately address the misconduct until it had been notified of the CME's investigation. In ordering the firm to pay a civil monetary penalty in the amount of $300,000, the CFTC recognized its cooperation, prompt acceptance of responsibility for the conduct at issue, and proactively implementing remedial measures and processes.

The continued development of the Division's self-reporting program, along with increased awareness and use of non-prosecution agreements, may result in more actions against corporate entities for failing to detect and deter spoofing. Additionally, the market surveillance unit previously housed within the CFTC's Division of Market Oversight now reports to the Director of the Division. This surveillance shift, along with the continued growth of the Division's Whistleblower Office, will likely result in an uptick in leads alleging potential spoofing activity. With increased scrutiny upon spoofing and disruptive trading, companies should ensure that sufficient compliance systems are in place to detect such trading activity. Finally, as the Division's investigations can be wide-ranging in scope, companies should be cognizant of potential supervision issues, as well as recordkeeping, reporting, and registration requirements.

Manipulation

Similarly, the Division's anti-manipulation program will continue to be active as it will likely expand into the virtual commodity space, and will be further driven by the Division's enhanced advisory, the use of non-prosecution agreements, and move of the surveillance unit to the Division.

As a result, the Division will continue to pursue allegations of potentially manipulative activity across all of the markets under its jurisdiction, ranging from virtual currencies, financial benchmarks, credit default swap indices, and other indices. Financial benchmark cases of

LIBOR and ISDA FIX will continue to be resolved in Fiscal Year 2018. So far this fiscal year, the Division settled cases against Statoil and Deutsche Bank:

- *In re Statoil ASA*, CFTC Dkt. No. 18-04 (Nov. 14, 2017)

The CFTC found that, from as early as October 2011 through November 2011, Statoil ASA ("Statoil") attempted to manipulate the Argus Far East Index ("FEI") of propane prices in order to benefit Statoil's physical and financial positions, including Statoil's NYMEX-cleared over-the-counter swaps which settled to the Argus FEI. Specifically, the CFTC found that Statoil sustained losses in its gas liquids unit throughout 2011, and after incurring those losses and in anticipation of seasonal market forces, Statoil established physical and financial positions that would benefit from a rising Argus FEI. The CFTC alleged that because the market conditions that Statoil expected never came to be, Statoil faced even greater potential losses as a result. To avoid these losses and meet customer obligations, the CFTC alleged that Statoil attempted to prop up the Argus FEI by purchasing propane cargo during the November Argus FEI propane price-setting window, hoping to signal that demand was high and to put pressure on the November Argus FEI propane price to increase. The CFTC imposed a $4 million civil monetary penalty.

- *In re Deutsche Bank Securities, Inc.*, CFTC Dkt. No. 18-09 (Feb. 1, 2018)

The CFTC found that, beginning in at least January 2007 and continuing through May 2012, Deutsche Bank Securities, Inc. ("DB") made false reports and, through the acts of multiple traders, attempted to manipulate the U.S. Dollar International Swaps and Derivatives Association Fix ("ISDAFIX"), a benchmark reference rate utilized in certain interest rate products, in order to benefit DB's derivatives positions, including positions involving cash-settled options on interest rate swaps. The CFTC found that DB bid, offered, and executed transactions in targeted interest rate products, including swap spreads and U.S. Treasuries, at or near 11:00 a.m., when the rate was set, or "fixed," to affect rates on the electronic interest rate swap screen and therefore increase or decrease the swaps brokers' reference rates and influence the final published ISDAFIX. The CFTC found that DB swaps traders, in a coordinated fashion over a period of years, would tell the swaps broker their need for a certain swap level at 11:00 a.m., or their need to have the level moved up or down. The CFTC imposed a $70 million civil monetary penalty against DB.

Cybersecurity

As noted by Chairman Giancarlo, "cybersecurity risks of hackable trading platforms and virtual currency wallets" are among the risks that are associated with virtual currencies. With the increase in cyberthreats targeting financial institutions, the Division likely will increase its scrutiny of surveillance systems at registered entities to ensure that the appropriate administrative, technical, and physical safeguards are in place to protect customer records and data. Entities registered with the CFTC should be proactive and ensure that their cybersecurity policies and systems adequately safeguard customer records and information

from cyberthreats. Even if these duties are delegated to third parties, registered entities are still required to diligently supervise the third parties to ensure full compliance with the CFTC's rules and regulations. Should a data breach occur, immediate remediation efforts and cooperation with the Division may help to reduce liability. So far in Fiscal Year 2018, the CFTC resolved the following action related to cybersecurity:

- *In re AMP Global Clearing LLC*, CFTC Dkt. No. 18-10 (Feb. 12, 2018)

The CFTC found that, since 2010, AMP Global Clearing LLC ("AMP"), a registered futures commission merchant, failed to diligently supervise the implementation of critical provisions in its information systems security program ("ISSP") between June 21, 2016 and April 17, 2017. As a result of this failure, a significant amount of AMP's customers' records and information were left unprotected for nearly ten months. In April 2017, a third party unaffiliated with AMP accessed AMP's information technology network and copied 97,000 files including customer records and information. The third party contacted the federal authorities about securing the copied information and informed AMP that the copied information was secured and no longer in the third party's possession. After becoming aware of the vulnerability and unauthorized access, AMP cooperated with the CFTC and worked diligently to remediate the issue. AMP was ordered to pay a civil monetary penalty in the amount of $100,000, and to provide two written follow-up reports within one year to the CFTC verifying its ongoing efforts to maintain and strengthen the security of its network and compliance with its ISSP's requirements.

Other matters

In addition to the areas described above, the Division continues to pursue other violations of the Commodity Exchange Act and CFTC Regulations. Companies should consider the Division's enhanced advisory and ensure that systems, policies, and procedures are robust. Examples of cases brought thus far include:

- *In re Glencore Agriculture B.V., f/k/a Glencore Grain B.V., and Glencore Ltd.*, CFTC Dkt. No. 18-12 (Apr. 30, 2018)

The CFTC found that, on multiple trading days during May 2013, June 2013, and June 2014, Glencore Grain B.V. and Glencore Ltd. held net positions in ICE Futures Cotton No. 2 contracts that, on an aggregated basis, exceeded the speculative limits established by the CFTC. The order stated that, on twenty-four occasions between January 2013 and November 2015, Glencore Grain B.V. and Glencore Ltd. executed exchange of futures for physical transactions opposite each other's cotton futures trading accounts, even though their accounts were not independently controlled as required for such transactions in order to not be considered illegal wash trades.

Additionally, on at least two occasions in 2013 and 2014, Glencore Grain B.V. submitted a Statement of Cash Positions in Cotton (CFTC Form 304) to the CFTC that failed to

accurately represent all required information, including its short cash sales commitments. Glencore B.V. and Glencore Ltd. were assessed, jointly and severally, a $2 million civil monetary penalty.

- *In re INTL FCStone Financial Inc. and FCStone Merchant Services LLC*, CFTC Dkt. No. 18-05 (Nov. 14, 2017)

The CFTC found that, on numerous occasions between December 2013 and March 2014, FC Stone Merchant LLC entered multiple noncompetitive trades, and against INTL FCStone Financial, a registered futures commission merchant, for reporting non-*bona fide* prices to the CME, where Canadian Dollar futures were exchanged for physical canola seed, which were not sufficiently related as required by the CME's rules. Because the futures trades were not executed competitively and were not in compliance with exchange rules governing exchange for related position transactions, the trades constituted "fictitious sales" and resulted in the reporting of non-*bona fide* prices. The CFTC also found that INTL FCStone Financial failed to have adequate compliance controls to identify exchange for related position transactions and did not have an adequate supervisory system in place for executing, handling, and reporting exchange for related position transactions. INTL FCStone Financial and FC Stone Merchant LLC were ordered, jointly and severally, to pay a civil monetary penalty in the amount of $280,000.

- *In re Cargill, Inc.*, CFTC Dkt. No. 18-03 (Nov. 6, 2017)

The CFTC found that Cargill, Inc. ("Cargill") deliberately provided inaccurate mid-market marks on swaps to counterparties and its swap data repository ("SDR"), which had the effect of concealing up to ninety percent of Cargill's full mark-up in violation of swap dealer business conduct and reporting requirements. Cargill was also determined to have failed to supervise its swap dealer employees, including by not having any systems or procedures in place that could have prevented or corrected its inaccurate communications about its grain marketing program and by not taking any steps to bring its marks into compliance prior to providing those marks to counterparties or the SDR. Cargill was ordered to pay a civil monetary penalty in the amount of $10 million.

- *In re Morgan Stanley and Co. Incorporated*, CFTC Dkt. No. 18-02 (Nov. 2, 2017)

The CFTC found that, from 2007 through 2017, Morgan Stanley and Co. Incorporated ("Morgan Stanley") omitted thousands of line items of information regarding mandatory futures and options transactions on the CME and Minneapolis Grain Exchange from its Part 17 Large Trader reports submitted to the CFTC due to problems with Morgan Stanley's proprietary reporting software. On account of Morgan Stanley's substantial cooperation, including proactively providing information about the scope and duration of the deficiencies and self-reporting an additional deficiency, promptly remediating the reporting deficiencies, as well as proactively implementing processes to ensure that the problems would not recur,

the civil monetary penalty imposed against Morgan Stanley was significantly reduced to the amount of $350,000.

Conclusion

Although the Division continues to operate under limited resources, further exacerbated by a recent budget cut, the first half of Fiscal Year 2018 shows that the Division's enforcement activity will continue to run full steam ahead for the remainder of the fiscal year. As the Division's Director has made clear his emphasis on self-reporting and cooperation, market participants would benefit by being proactive, remediating issues immediately, and meaningfully engaging with the Division. Additionally, compliance personnel should ensure that their surveillance systems, compliance policies and procedures, and adequate safeguards are in place, and ensure that any deficiencies are remediated upon detection.

0.00 avg. rating (**0**% score) - **0** votes

(1d)

--